UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,982	08/29/2001	Takashi Endo	NIT-295	5993

24956 7590 11/05/2009
MATTINGLY & MALUR, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
11/05/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.**
	09/940,982
		Applicant(s)
		ENDO ET AL.	

	Examiner Zachary A. Davis	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _17 September 2009_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1,3 and 28_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1,3 and 28_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 24 July 2009 has been received but was not fully compliant with the provisions of 37 CFR 1.121 as detailed in the notice of non-compliant amendment mailed 18 August 2009.

2. A response to the notice of non-compliant amendment was received on 17 September 2009 and has been entered. By this response, Claim 1 has been amended. Claims 2, 4-8, 18, 20-22, and 24-27 have been canceled. New Claim 28 has been added. Claims 1, 3, and 28 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments filed 24 July 2009 have been fully considered but they are not persuasive.

Regarding the rejection of the claims under 35 U.S.C. 103(a) as unpatentable over Applicant admitted prior art in view of Jaffe et al, US Patent 6510518, and with specific reference to independent Claims 1 and 28, Applicant argues that the combination of the admitted prior art and Jaffe would not be considered by one of ordinary skill in the art.

More specifically, Applicant asserts that application of the constant Hamming weight representation as taught by Jaffe to data in the admitted prior art apparatus would double the amount of data to be processed (page 7 of the present 24 July 2009 response) and that therefore a circuit of twice the size or scale must be used, which would be a disadvantage (page 7 of the present response). However, the Examiner notes that this is not necessarily the case, and that doubling the amount of data would not necessarily require twice the size of the circuitry, but could also be achieved, for example, by the same circuitry but with an increase in the amount of processing time required. While the Examiner recognizes that decreased processing speed or increased size of circuitry would be a disadvantage, the techniques of Jaffe also provide a substantial advantage, namely the increase in security provided by the minimization of information leaked by power consumption fluctuations (see Jaffe, column 2, lines 44-48, as previously cited). The Examiner submits that one of ordinary skill in the art would have at least considered the teachings of Jaffe and considered that the tradeoff between security and speed or size may be such that it would nevertheless be beneficial to incorporate the teachings of Jaffe. It is further noted that Jaffe additionally contemplated hardware implementations that could potentially be optimized for less space and faster performance when implementing the teachings therein (see column 11, line 59-column 12, line 19).

Applicant further asserts that "neither the disturbance data XI nor the disturbance data XO is obtained by using the first and second disturbance data of AAPA and a constant Hamming weight representation as taught by Jaffe. If the first and second disturbance data of AAPA are applied by [sic] a constant Hamming weight representation taught by Jaffe, the second disturbance data obtained by using a processing operation on the first disturbance data of AAPA may not securely prevent the Hamming weight of disturbance data XI from becoming 0 or 8, which leaves a potential security hole" (pages 7-8 of the present response). The Examiner fails to appreciate this argument; it is unclear how the second sentence follows from the first. Additionally, to the extent that the Examiner understands Applicant's argument to suggest that the use of Jaffe's constant Hamming weight representation for the first disturbance data XI would not necessarily make the second disturbance data XO also have a constant Hamming weight, the Examiner notes that Applicant's assertion amounts to conjecture and would appear to contradict the teachings of Jaffe. The Examiner submits that, as previously noted, the teachings of Jaffe suggest that the constant Hamming weight representation would be used on all data in a system (see Jaffe, column 2, lines 56-60, as previously cited). Further, any processing performed on the first disturbance data to obtain the second disturbance data would not affect the Hamming weight of any of the disturbance data if all data were in a constant Hamming weight representation as taught by Jaffe. The representations of Jaffe make it so that all data has exactly half of the bits as zeros and the remaining bits as ones (see Jaffe, column 4, line 55-column 5, line 30, as previously cited). Any processing performed on such data would still result in an equal number of ones and zeros in the data (i.e. a constant Hamming weight). It is noted that Applicant has not provided any evidence in support of the allegation that this representation nevertheless “may not securely prevent the Hamming weight… from becoming 0 or 8” as alleged (page 7 of the present response) even though Jaffe explicitly describes the representations as always having constant Hamming weight (column 4, line 55-column 5, line 30; column 2, lines 56-60) in order to minimize the information leaked from cryptographic systems by power consumption fluctuations (see Jaffe, column 2, lines 44-48). This is in direct contrast to Applicant’s allegation that this opens a potential security hole due to observation of the current consumption (pages 7-8 of the present response), as Jaffe explicitly states that the constant Hamming weight representation and the other techniques taught therein are particularly for the purpose of reducing or eliminating leakage of information due to measurement of power consumption (i.e. current consumption, see Jaffe, column 2, lines 44-56). Therefore, again, the Examiner fails to appreciate Applicant’s argument.

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Specification

4. The objection to the specification for failure to provide proper antecedent basis for the claimed subject matter is NOT withdrawn; although the amendments to the

claims have overcome the previous issues, the amendments also raise new issues as detailed below.

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 1 has been amended to recite the limitation “a table of candidates of disturbance data XI”, and new Claim 28 recites the similar limitation “a table of candidate pairs of disturbance data XI and disturbance data XO”. There does not appear to be sufficient antecedent basis for these limitations in the present specification, nor does there appear to be any mention of tables of candidates of disturbance data (or pairs thereof) in the specification. For further detail, see below regarding the rejection under 35 U.S.C. 112, first paragraph, for failure to comply with the written description requirement.

Claim Rejections - 35 USC § 112

6. The rejection of Claims 2 and 4-8 under 35 U.S.C. 112, first paragraph, for failure to comply with the written description requirement is moot in light of the cancellation of the claims. The rejection of Claims 1 and 3 is NOT withdrawn; although the amendments to the claims have addressed the previous issues, the amendments have also raised new issues with respect to the written description requirement, as set forth below.

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1, 3, and 28 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 1 has been amended to recite the limitation “a table of candidates of disturbance data XI”, and new Claim 28 recites the similar limitation “a table of candidate pairs of disturbance data XI and disturbance data XO”. Applicant has not pointed out where the new and amended claims are supported, nor does there appear to be sufficient written description of the above claim limitations in the application as filed. There does not appear to be any mention of tables of candidates of disturbance data (or pairs thereof) in the present specification. See MPEP § 2163.04(I)(B).

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1, 3, and 28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation “a memory holding a table of candidates of disturbance data XI which maintains a constant Hamming weight before and after processing said disturbance data XI with said predetermined processing OP1" in lines 5-7. It is unclear what the phrase "which maintains a constant Hamming weight" is intended to modify. It appears that it may be intended to modify all of the candidates of disturbance data, but if this is the case, then the verb "maintains" does not agree with the intended subject. Further, the phrase "said disturbance data" in lines 6-7 and also recited in line 8 does not have sufficient antecedent basis. The table of candidates of disturbance data appears to refer to multiple items of disturbance data, and therefore it is unclear to which disturbance data the limitation is intended to refer. The claim further recites a means for "performing said predetermined processing OP1 on said input data D1, or a processing different from said predetermined processing OP1 on said transformed data H1, in order to generate processed transformed data H2" in lines 16-20 of the claim. However, if the processing is performed on data D1 as recited in the first phrase, it is not clear how the output would result in "processed transformed data" as claimed when the data D1 has not been transformed (as opposed to transformed data H1). All of the above renders the claim indefinite.

Claim 3 also recites "said disturbance data" in lines 2-3. It is unclear to which of the multiple items of disturbance data (recited in Claim 1, line 5) this is intended to refer.

Claim 28 recites the limitation "said disturbance data XI" in lines 6 and 7. However, the claim also recites multiple candidate pairs of disturbance data XI and XO in line 5, and it is not clear to which of these multiple items of disturbance data XI these limitations are intended to refer. Claim 28 also recites "said processing said disturbance data XI" in line 9; this is generally unclear, as it is not clear to what processing this is intended to refer. Further, the claim recites “said disturbance data XI of a pair of said disturbance data XI and XO selected by said selector” in lines 12-14. Although it appears that this may be intended to refer to the pair of disturbance data selected in line 11, the use of “a pair” (instead of “the pair” or “said pair”) makes it unclear if this is intended to refer to the same pair of disturbance data. Claim 28 further recites a means for “performing said predetermined processing OP1 on said input data D1, or a processing different from said predetermined processing OP1 on said transformed data H1, in order to generate processed transformed data H2” in lines 15-18 of the claim. However, if the processing is performed on data D1 as recited in the first phrase, it is not clear how the output would result in “processed transformed data” as claimed when the data D1 has not been transformed (as opposed to transformed data H1). All of the above renders the claim indefinite.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1, 3, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

In reference to Claim 1, Applicant admits as prior art an apparatus including a selector for selecting disturbance data; disturbance data processing means performing predetermined processing on the selected disturbance data to generate processed disturbance data; a data transform means transforming input data by using the selected disturbance data to generate transformed data; a transformed data processing means for performing predetermined processing on the transformed data to generate processed transformed data; and a data inverse transform means for performing inverse transformation processing on the processed transformed data using the processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60) and further discloses the use of look-up tables as basic operations, for example in cryptographic systems (see column 15, line 61-column 16, line 14, noting that it is well-known that table lookups of pre-computed values can increase processing speed). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order to minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45, and column 5, lines 12-18).

In reference to Claim 28, Applicant admits as prior art an apparatus including a selector for selecting disturbance data and that processed disturbance data is obtained by performing predetermined processing on the selected disturbance data; a data transform means transforming input data by using the selected disturbance data to generate transformed data; a transformed data processing means for performing predetermined processing on the transformed data to generate processed transformed data; and a data inverse transform means for performing inverse transformation processing on the processed transformed data using the processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60) and further discloses the use of look-up tables as basic operations, for example in cryptographic systems (see column 15, line 61-column 16, line 14, noting that it is well-known that table lookups of pre-computed values can increase processing speed). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order to minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Ikeda, US Patent 4334273; Miyakawa et al, US Patent 4783829; Floro, US Patent 5410717; Dent, US Patent 5577053; Salamon, US Patent 6011566; and Adachi, US Patent 6111982, for example, among others, each generally disclose the use of look-up tables in place of more complicated processing operations.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Examiner, Art Unit 2437